SECTION II—CLAIMS

1.-36. (Canceled)

37.   (New) A method comprising:

   receiving from a terminal a first request including a composite address, the composite address including an unencrypted address of a secure server with an encrypted address of a web page concatenated thereto;

   transmitting a second request to a web site containing the web page, wherein the second request alters or omits an address of the terminal;

   retrieving the web page designated in the second request;

   modifying an address associated with the retrieved web page so that the secure server appears to be the source of the web page; and

   encrypting the content of the retrieved web page and sending the encrypted web page, via a secure link, to the terminal.

38.   (New) The method of claim 37 wherein the secure link comprises a secure sockets layer (SSL) link.

39.   (New) The method of claim 37 wherein modifying the address associated with the retrieved web page comprises modifying a Uniform Resource Locator (URL) or Internet Protocol (IP) address of the web site.

40.   (New) The method of claim 37 wherein modifying the address associated with the retrieved web page comprises modifying an address associated with a hypertext link in the retrieved web page to indicate the address associated with the secure server.

41.   (New) The method of claim 37, further comprising modifying computer code associated with the retrieved web page to cause subsequent requests related to the retrieved web page to be sent by the terminal to the secure server instead of to the web site.

42.   (New) The method of claim 37, further comprising decrypting the encrypted address of the web page.

43.   (New) The method of claim 37, further comprising repeating the retrieving, modifying, encrypting, and sending while the secure link is active.

44.   (New) The method of claim 37, further comprising triggering a deletion of stored electronic files at the terminal related to a communication via the secure link, in response to termination of the communication between the terminal and the secure server.

45.   (New) The method of claim 37, further comprising, at the secure server, controlling transmission of electronic files to the terminal based on preferences received from the terminal.

46.   (New) The method of claim 37, further comprising storing under a pseudonym at a location communicatively coupled to the secure server, electronic files sent with the web page.

47.   (New) The method of claim 37, further comprising:

    obtaining information related to a user's communication with the secure server;

    providing the obtained information to an entity based on permission of the user and in exchange for providing the secure link; and

    providing advertisements from the entity to the user related to the obtained information.

48.   (New) A machine-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to effect the following:

    receive from a terminal a first request including a composite address, the composite address including an unencrypted address of a secure server with an encrypted address of a web page concatenated thereto;

    transmit a second request to a web site containing the web page, wherein the second request alters or omits an address of the terminal;

    retrieve the web page designated in the second request;

    modify an address associated with the retrieved web page so that it appears that the secure server is the source of the web page; and

    encrypt the content of the retrieved web page and sending the encrypted web page, via a secure link, to the terminal.

49. (New) The machine-readable medium of claim 48 wherein the instructions cause the processor to send the encrypted data via the secure link by sending the encrypted data via a secure dockets layer (SSL) link.

50. (New) The machine-readable medium of claim 48 wherein the instructions cause the processor to modify the address associated with the retrieved web page by modifying a Uniform Resource Locator (URL) or Internet Protocol (IP) address of the web site.

51. (New) The machine-readable medium of claim 48 wherein the instructions cause the processor to:

receive the request from the terminal forwarded from an intermediate unit;

retrieve the web page designated in the request from a source;

modify address information in the retrieved web page to indicate a source address corresponding to an address associated with the intermediate unit rather than to an address associated with the source that provided the web page; and

directly send an encrypted version of the retrieved web page from the secure server to the terminal, via the source link.

52 (New) An apparatus comprising:

a processor coupled to a storage unit, the storage unit being capable of storing a computer program; and

a communication unit to allow the processor to communicate with a terminal and with a web site, wherein the computer program is capable of directing the processor and the communication unit to:

receive from the terminal a first request including a composite address, the composite address including an unencrypted address of a secure server with an encrypted address of a web page concatenated thereto;

transmit a second request to the web site, wherein the second request alters or omits an address of the terminal;

retrieve the web page designated in the second request;

modify an address associated with the retrieved web page so that the secure server appears to be the source of the web page; and

encrypt the content of the retrieved web page and sending the encrypted web page, via a secure link, to the terminal.

53.   (New) The apparatus of claim 52 wherein the secure link comprises a secure sockets layer (SSL) link.

54.   (New) The apparatus of claim 52, further comprising a database unit communicatively coupled to the processor to store electronic files under a pseudonym, the electronic files corresponding to data sent from the web site along with the retrieved web page.

55.   (New) A method comprising:

receiving at an intermediate unit a first request from a terminal including a composite address, the address including an unencrypted address of a secure server with an encrypted address of a web page concatenated thereto;

forwarding the first request to the secure server;

transmitting a second request to a web site containing the web page, wherein the second request includes the web page address and alters or omits an address of the terminal;

retrieving the web page designated in the second request;

modifying an address associated with the retrieved web page so that the intermediate unit appears to be the source of the web page; and

encrypting the content of the retrieved web page and sending the encrypted web page, via a secure link, from the secure server to the terminal.

56.   (New) The method of claim 55, further comprising receiving, at the secure server, communication protocol information related to a communication between the terminal and the intermediate unit, to allow the secure server to respond to requests sent to the intermediate unit from the terminal.

57.   (New) The method of claim 55 further comprising receiving subsequent requests from the terminal at the intermediate unit rather than directly at the secure server from the terminal.

58.   (New) The method of claim 55, further comprising decrypting the encrypted web page address.

59. (New) The method of claim 58, further comprising re-encrypting the address associated with the retrieved web page and concatenating the re-encrypted address with the address associated with the intermediate unit.

60. (New) A machine-readable medium having stored thereon instructions, which when executed by a processor cause the processor to effect the following:

receive at an intermediate unit a first request from a terminal including a composite address, the composite address including an unencrypted address of a secure server with an encrypted address of a web page concatenated thereto;

forward the first request to the secure server;

transmit a second request to a web site containing the web page, wherein the second request includes the web page address and alters or omits an address of the terminal;

retrieve the web page designated in the second request;

modify an address associated with the retrieved web page so that it appears that the intermediate unit is the source of the web page; and

encrypt the content of the retrieved web page and sending the encrypted web page, via a secure link, from the secure server to the terminal.

61. (New) The machine-readable medium of claim 60, further comprising instructions to receive, at the secure server, communication protocol information related to a communication between the terminal and the intermediate unit, to allow the secure server to respond to requests sent to the intermediate unit from the terminal.

62. (New) The machine-readable medium of claim 60, further comprising instructions to receive subsequent requests from the terminal at the intermediate unit rather than directly at the secure server from the terminal.

63. (New) The machine-readable medium of claim 60, further comprising instructions to decrypt the encrypted web page address.

64. (New) The machine-readable medium of claim 63, further comprising instructions to re-encrypt the address associated with the retrieved web page and concatenating the re-encrypted address with the address associated with the intermediate unit.

65.   (New) An apparatus comprising:

a first server including a processor coupled to a storage unit, the storage unit being capable of storing a first computer program;

a secure second server including a processor coupled to a storage unit, the storage unit being capable of storing a second computer program;

a first communication unit in the first server, wherein the first communication unit allow the first server to communicate with a terminal and with the second server, wherein the first computer program is capable of directing the processor and the communication unit to:

receive a first request from the terminal including an address, the address including an unencrypted address of the second server with an encrypted web page address concatenated thereto, and

forward the first request to the second server; and

retrieve the web page designated in the second request,

modify an address associated with the retrieved web page so that first server appears to be the source of the web page, and

encrypt the content of the retrieved web page and send the encrypted web page, via a secure link, from the second server to the terminal.

66.   (New) The apparatus of claim 65 wherein the secure server receives communication protocol information related to a communication between the terminal and the first server, to allow the secure server to respond to requests sent to the intermediate unit from the terminal.

67.   (New) The apparatus of claim 65 wherein the first server receives subsequent requests from the terminal rather than the second server.

68.   (New) The apparatus of claim 65 wherein the second server decrypts the encrypted web page address.

69.   (New) The apparatus of claim 68 wherein the second server re-encrypts the address associated with the web page and concatenates the re-encrypted address with the address associated with the first server.